Design of a Pseudo-Random Binary Code Generator via a Developed Simulation Model

A. Ahmad and D. Al-Abri
Department of Electrical and Computer Engineering
College of Engineering, Sultan Qaboos University
P. O. Box 33, Postal Code 123; Muscat, Sultanate of Oman
Tel.: (968) 2414 1327; Fax. (968) 2441 3416
E-mails afaq@squ.edu.om; alabrid@squ.edu.om

***Abstract*—This paper presents a developed tool for Pseudo-Random Binary Code generator (PRBCG). Based on extensive study of LFSR theory we developed the simulation model of PRBCG. The developed model is faster and simulates the process for very high length of Linear Feedback Shift Registers (LFSRs). We tested our model for the value n = 300 where n is the length of the LFSR. The developed software model is also capable of providing the transition states of different bits of LFSRs. Further, the model has capability of switching to any possible characteristic polynomial (feedback connections) of n-bit LFSR. Also, the model is designed such that it can accommodate all the possible initial conditions (2^n) of LFSR.**

***Index Terms*— Pseudo-Random Binary Code, Linear Feedback Shift Registers, Generating Function, Feedback Connection, Initial Condition, m-sequence**

I. Introduction

Pseudo-Random Binary Code (PRBC) is widely used in modern engineering. The generation of PRBCs and study of their properties has attained the more and more attention of the researchers because of its wide applications. Therefore, how to design the Linear Feedback Shift Register (LFSR) based hardware circuit to generate PRBCs. Moreover, the PRBC sequence o the longest cycle is popularly known as Maximal Length PRBC sequence (m-sequence). The m-sequence which is one of the basic sequences has always been topic of current research.

Linear Feedback Shift Registers (LFSRs) have been used for Pseudo-Random Binary Code Sequence (PRBCS) generation. The PRRBSs have been used for multiple uses in digital systems design. Applications include cryptographic applications like stream ciphers and data hiding. The concept of LFSR theory is useful in many error correction and detection codes. The PRRBSs have been used in Built-In Self-Testing (BIST) for VLSI circuits [1] – [19]. Many more application of LFSR and PRBCS can be listed as given below:

- Wireless Communications
- Data Integrity
- Checksums
- Data Compression
- Pseudo-random Number Generation (PN)
- Direct Sequence Spread Spectrum
- Scrambler/Descrambler
- Optimized Counters

In this paper we present a developed simulated tool which is capable of generating PRBC efficiently. The developed tool is culmination of exhaustive study of LFSR theory. Therefore, in the ensuing section first we briefly present the mathematical modeling of LFSR.

II. Mathematical model of linear feedback shift register

There exist many LFSR models. The classifications of LFSR models are based on the placements of the Exclusive-OR circuits and the shifts of the registers. The classifications on basis of shifts are right to left or left to right. Also, the shift is considered from the first bit to last bit or from last bit to the first bit. Similarly, the classifications of LFSRs on the basis of Exclusive-OR circuits are recognized as External Exclusive-OR (EEOR) or as Internal Exclusive-OR (IEOR). Figure 1 depicts an n-bit LFSR circuit. This structure is based on External Exclusive-OR circuits. The shift register shifts the data from bit n to bit 1 while the feedback taps vector [c_0, c_1, . . . c_n]. The feedback taps c_1, c_2, . . c_n are linked with flip-flop's outputs Q_n, Q_{n-1}, . . Q_2, Q_1 respectively whereas c_0 link represents the connection between the output of EEOR circuits and the input of the flip-flop n. The state space model of this LFSR can be described as follows.

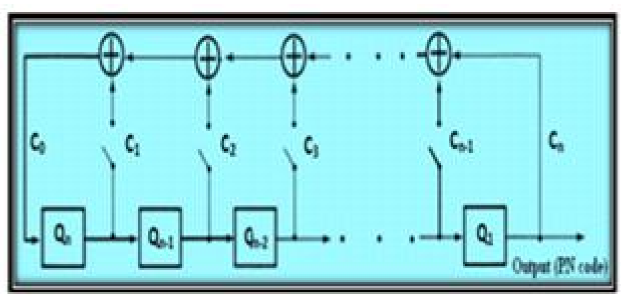

Figure 1. An n-bit LFSR

The state space model of this LFSR structure can be described as given in equation (1). To explain let matrix [A] represent the state transition matrix of order n × n, for an n stage LFSR shown in Fig. 1. Let the state at any time 't' be represented by vector [Q(t)] = [$Q_n(t)$, ... ,$Q_j(t)$, ... ,$Q_2(t)$, $Q_1(t)$] (which is effectively the contents of the LFSR) where each Q_j represents the state of the j^{th} stage of the LFSR. Further, let the LFSR feedback stages be numbered from C0 to Cn, proceeding in the same direction as the shifting occurs i.e.

DOI: 01.IJIT.02.01. 53

left to right. Let the present state of the LFSR be represented by [Q(t)] and, one clock later, the next state by [Q(t+1)]; then the relationship between the two states is given by as described in equation (1).

$$\begin{bmatrix} Q_n(t+1) \\ Q_{n-1}(t+1) \\ Q_{n-2}(t+1) \\ \vdots \\ Q_2(t+1) \\ Q_1(t+1) \end{bmatrix} = \begin{bmatrix} c_n & c_{n-1} & \cdots & c_2 & c_1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} Q_n(t) \\ Q_{n-1}(t) \\ Q_{n-2}(t) \\ \vdots \\ Q_2(t) \\ Q_1(t) \end{bmatrix} \quad (1)$$

Where, $c_j = 0$ or 1, for $1 \leq j \leq n-1$ and $c_j = 1$, for j = 0, n.

In equation (1), the values of c_j show the existence or presence of a feedback connection from the j^{th} stage of the LFSR. Thus the state equation for this model can be given as in equation (2).

$$[Q(t+1)] = [A] * [Q(t)] \quad (2)$$

If [Q] = [Q(0)] represents a particular initial loading of the LFSR, i.e. the content of each flip-flop is zero. Then the sequence of states through which the LFSR will pass will all the time zeros; means the LFSR is locked. Otherwise, for any other loadings the LFSR will be governed by equation (3) during its successive operation times.

$$[Q(t)],\ [A][Q(t)],\ [A]^2[Q(t)],\ [A]^3[Q(t)],.. \quad (3)$$

Let the matrix 'period' be the smallest integer p for which $[A]^p = I$, where I is an identity matrix. Then $[A]^p[Q(t)] = [Q(t)]$ for any non zero initial vector [Q(0)], indicating the 'cycle length (or period)' of the LFSR is p. As mentioned above the cycle length for [Q(0)] = 0 is always 1, independent of matrix [A]. Thus, on the basis of this property of periodicity of LFSR and equation (4), it follows that.

$$[Q(t)] = [Q(t+p)] = [A]^p[Q(t)] \quad (4)$$

To demonstrate equation (4) and to verify its existence let us consider an example as below. Example 1: Consider a 3-bit LFSR as shown in Fig. (2). The LFSR has feedback connections as $c_0 = c_1 = c_3 = 1$ and $c_2 = 0$. It can be verified by the by using equations (1) and (4) that this LFSR structure has period of 7.

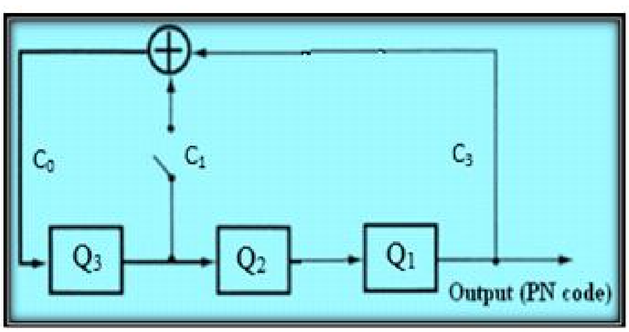

Figure 2. A 3-bit LFSR

Table I demonstrates the all possible sequences of states through which this LFSR structure passes before repeating the initial loading. The LFSR is loaded with all 1's content.

TABLE I. THE OPERATION OF LFSR OF EXAPLE 1

States			Comments
Q_3	Q_2	Q_1	
1	1	1	Initial
0	1	1	
1	0	1	
0	1	0	
0	0	1	
1	0	0	
1	1	0	
1	1	1	Repeats after a period p = 7

Any binary data sequence can be represented in form of polynomial in GF(2). Therefore, the tap vector for an LFSR can be represented in the form of polynomial and is technically known as characteristic polynomial. Equations (5) define a general form of characteristic polynomial and let us call it as P(x).

$$P(x) = \sum_{i=0}^{n} (c_i x^i) \quad (5)$$

Let $\{a_m\} = [a_0, a_1, \ldots, a_i, \ldots]$, represent the output sequence generated by the LFSR used as PRBCS, where $a_i = 0$ or 1. Then this sequence can be represented as as given in equation (6).

$$G(x) = \sum_{m=0}^{\infty} (a_m x^m) \quad (6)$$

From the structure of the type of the LFSR shown in Fig. 1, it can be seen that if the current state of the i^{th} flip-flop is a_{m-i}, for i = 1, 2 , ... , n , then by the recurrence relation an equation can be given as below.

$$a_m = \sum_{i=1}^{n} (c_i a_{m-i}) \quad (7)$$

The generating function G(x) associated with the PRBCS can be mathematically defined as in equation (8).

$$G(x) = \sum_{i=0}^{\infty} a_i x^i \quad (8)$$

Or,

$$G(x) = \frac{\sum_{i=0}^{n-1} x^i \sum_{k=0}^{i} c_k a_{i-k}}{\sum_{i=0}^{n} c_i x^i} \quad (9)$$

Or, equation (9) can be rewritten as:

$$G(x) = \frac{N(x)}{P(x)} \quad (10)$$

DOI: 01.IJIT.02.01.53

III. About the development and testing of the simulated model

To develop this simulation model we used Microsoft Visual Basic .Net programming environment is used to create graphical user application for the Microsoft Windows system. The theory of LFSR discussed in the above sections are embedded in this developed simulation model. In our developed simulation model where the general structure of LFSR model is programmed to target the objective of generating PRBCS. Requesting immediate after the size of an LFSR it generates lists of all possible polynomials for feedback connections and initial loadings. Immediate after the initial loading and feedback options are selected the developed tool computes and outputs the PRBCS. Our simulation model also has provision of controlling the length of the PRBCS.
Just to elaborate to the readers we present a model demonstration for data of example 1. The execution of the program outputs the first window which is shown in Fig. 3.

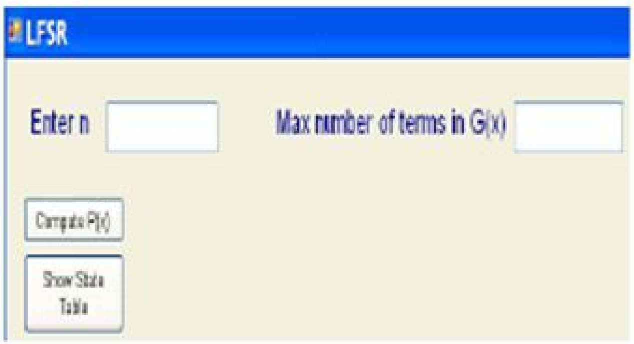

Figure 3: The first window of Model “LFSR”

Immediate after feeding the value n = 3 it generates functional windows for selecting P(x) and initial loadings as depicted in Fig. 4.

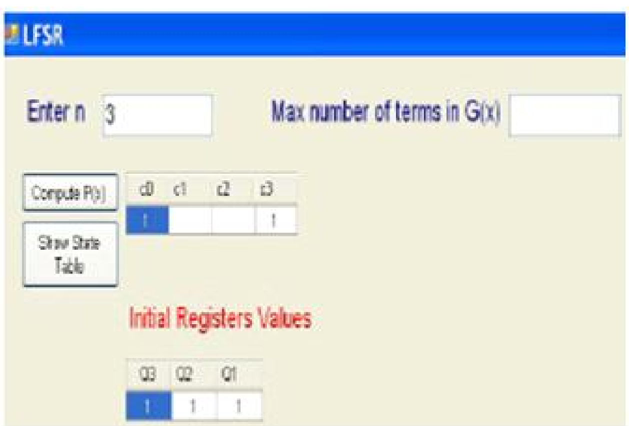

Figure 4: Selection window for the options of P(x) and initial loadings of Model “LFSR”

We can control the length of the generated sequence. As shown in Fig. 5 that for n = 3, with desired sequence length of 12, initial state loading of [1, 1, 1] and P(x) = ([1, 1, 0, 1] = 1 + x + x^3) that PRBCS repeats after the period of 7. It can also be visualized that maximum 12 terms of G(x) are computed. Our model provides the complete state table for the complete operation of generating PRBCS. Also, each G(x) and N(x) are

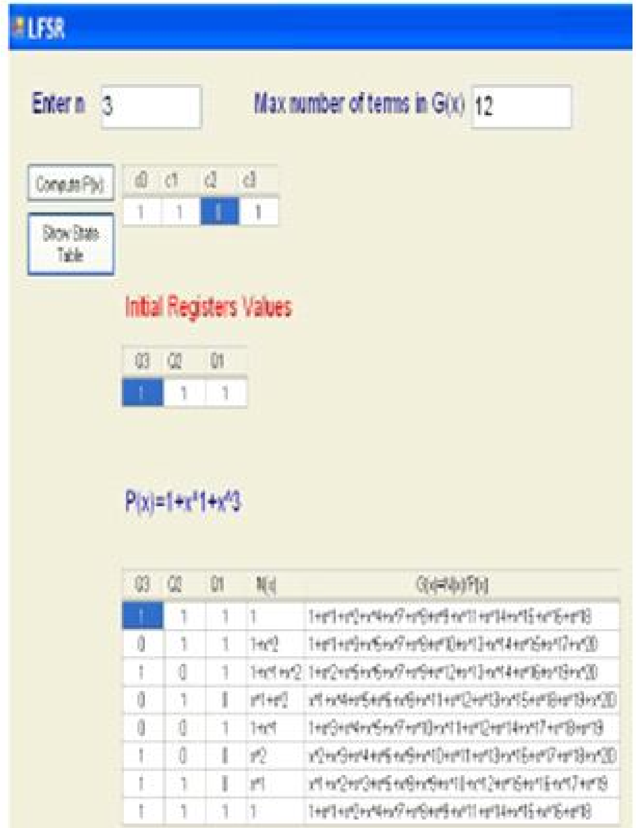

Figure 5: The output for n =3

computed and results are available in the window. These results can also be stored in files.

We tested our model for n = 300 but it is difficult to show the result. A partial window for n = 300 is shown in Fig. 6.

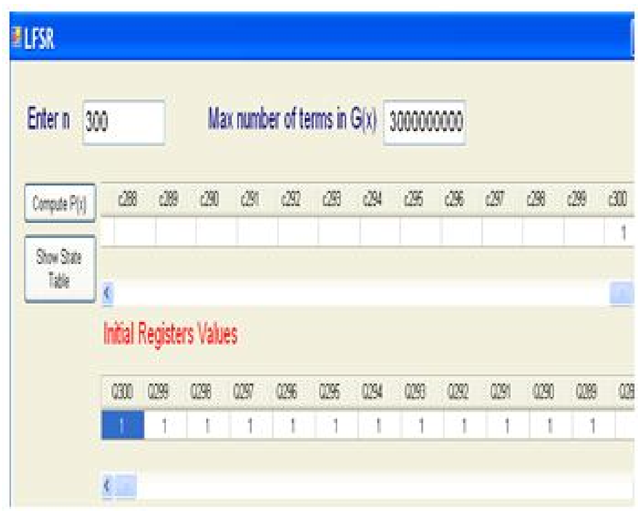

Figure 6: Simulated Window for n = 300

Conclusions

This work is based on the study of the theory of LFSR. Hence this tool is developed after a comprehensive study of LFSR theory and its related issues. First we tested our model for many values of n. We verified our models for small sizes of n. We also demonstrated and executed this model for n up to 300 and it runs satisfactorily. This developed tool requires

DOI: 01.IJIT.02.01. 53

a very small memory space and execution time is also less. During the test and execution of this developed model we never faced the problem of hanging of computer. Also, the output file can be exported either in EXCEL, MATLAB, C and FORTRAN 95.

ACKNOWLEDGMENT

The authors wish to thank and acknowledge the support grant (SQU-DVC/ PSR/RAID/2010/23) provided by Sultan Qaboos University, Sultanate of Oman.

REFERENCES

[1] Golomb, S.W., "Shift Register Sequences. *Aegean Park Press,"* Leguna Hills - U.S.A., 1982

[2] Ahmad A., Nanda N.K. and Garg K., "A critical role of primitive polynomials in an LFSR based testing technique," *IEE Electronics Letters (UK),* vol.24, no.15, 1988, pp. 953 – 955, 1988

[3] Ahmad, A., Nanda, N. K. and Garg, K., "The use of irreducible characteristic polynomials in an LFSR based testing of digital circuits," *Proceedings of 4th IEEE international conference of region 10 (TENCON-89),* pp. 494 – 496 1989

[4] Ahmad A., Nanda N.K. and Garg K., "Are primitive polynomials always best in signature analysis?" *IEEE design & Test of Computers (USA), 1990,* vol.7, no.4, pp. 36 – 38, 1990

[5] Ahmad, A., Nanda, N. K., and Garg, K., "An efficient design of maximal length of pseudorandom test pattern generators," *Proceedings of IEEE international conference on signals & systems, held at Ail-Ain (UAE),* Jan. 29 - 31, vol.1, pp. 27 – 34, 1990

[6] Ahmad A. and Elabdalla A. M., "An efficient method to determine linear feedback connections in shift registers that generate maximal length pseudo-random up and down binary sequences," *Computer & Electrical Engineering - An Int'l Journal (USA),* vol. 23, no. 1, pp. 33-39, 1997

[7] Ahmad, A., Al-Musharafi, M.J., and Al-Busaidi S., "A new algorithmic procedure to test m-sequences generating feedback connections of stream cipher's LFSRs," *Proceedings IEEE conference on electrical and electronic technology (TENCON'01),* vo. 1, pp. 366 – 369, 2001

[8] Ahmad, A., Al-Musharafi, M.J., and Al-Busaidi S., Al-Naamany, A. M., and Jervase, A. J., "An NLFSR based sequence generator for stream ciphers," *Proceedings (SETA'01) - An International Conference on Sequences & Their Applications,* pp. 11 – 13, 2001

[9] Jamil, T. and Ahmad, A., "An investigation in to the application of linear feedback shift registers for steganography," *Proceedings IEEE SoutheastCon2002, Columbia, SC, USA,* April 5 – 7, 2002, pp. 239 – 244, 2002

[10] Ahmad A., Al-Musharafi, M. J., Al-Busaidi, S., "Design and study of a strong stream crypto-system model for e-commerce," *International Council for Computer Communication Publishers, Washington DC, USA (The ACM Library),* vol. 1, pp. 619 – 630, 2002

[11] Ahmad, A., Development of State Model Theory for External Exclusive NOR Type LFSR Structures, *Enformatika,* vol. 10, pp. 125 – 129, 2005

[12] Ball, J.R., Spittle, A.H., Liu, H.T., "High-speed m sequence generation: a further note," *Electronics Letters,* vol. 11, no. 5, pp. 107 – 108, 11 July 2007

[13] Ahmad, A., "Investigation of Typical Properties of Some LFSR Structures," *Journal of System Science and Engineering,* vol. 17, no. 1, pp. 65 – 69, 2008

[14] Ahmad, A., and Al-Maashri, A., "Investigating Some Special Sequence Length Generated Through an External Exclusive-NOR Type LFSRs," *International Journal Electrical and Computer Engineering, (PERGAMON, Elsevier Science),* vol. 34, pp. 270 – 280, 2008

[15] Ahmad, A., Al-Mashari, A. and Al-Lawati, A. J., "On Locking Conditions in M-Sequence Generators for the Use in Digital Watermarking", *Proceedings International Conference on Methods and Models in Computer Science (ICM2CS09),* pp. 111 – 115, 2009

[16] Fangfang Cheng, Jingyu Hua, Jiaxiang Zhu, Lei Tong and Liming Meng, "A Fast Generation Method of Bent Sequences and Its Application in ADS Simulation," *Proceedings Wase international conference on information engineering (ICIE-2010),* pp. 328 – 331, 2010

[17] Junying Sun and Jiaxing Chen, "Design of m sequence generator based on protues," *Proceedings international conference on computer, mechatronics, control and electronic engineering (CMCE),* pp. 126 – 128, 2010

[18] Ahmad, A., "A Simulation Experiment on a Built-In Self Test Equipped with Pseudorandom Test Pattern Generator and Multi-Input Shift Register (MISR)", *International journal of VLSI design & Communication Systems (VLSICS),* vol.1, No.4, 2010

[19] A. Ahmad and L. Hayat, "Selection of polynomials for cyclic redundancy check for the use of high speed embedded systems – An algorithmic procedure", *WSEAS Transactions on Computers,* vol. 10, no. 1, pp. 16 – 20, 2011

DOI: 01.IJIT.02.01.53